

**THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION**

SOFTEX LLC

Plaintiff,

v.

**ABSOLUTE SOFTWARE CORPORATION
AND ABSOLUTE SOFTWARE, INC.**

Defendants.

Civil Action No. 1:22-cv-01308-DAE

JURY TRIAL DEMANDED

PLAINTIFF SOFTEX LLC'S RESPONSIVE CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE PATENTED TECHNOLOGY	1
III.	ARGUMENT	2
A.	“basic input/output system (BIOS)” / “BIOS”	2
B.	“power on self test (POST)”	4
C.	“hidden partition”	5
D.	“operating correctly” / “operated correctly”	7
E.	The “wherein integrating” terms	8
F.	“primary server”/ “central server”	9
G.	“changeable area” / “system area” / “non-volatile storage device” / “non-volatile memory”	10
H.	The Component/Module Terms	11
1.	35 U.S.C. §112, Sixth Paragraph, Does Not Apply	11
2.	If the Court Finds That §112, Sixth Paragraph, Does Apply:	16
3.	No Claim Term Is Indefinite	17
IV.	CONCLUSION	20

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>ABS Glob., Inc. v. Cytonome/St, LLC</i> , 84 F.4th 1034 (Fed. Cir. 2023)	10
<i>Baldwin Graphic Sys., Inc. v. Siebert, Inc.</i> , 512 F.3d 1338 (Fed. Cir. 2008).....	9
<i>BASF Corp. v. Johnson Matthey Inc.</i> , 875 F.3d 1360 (Fed. Cir. 2017).....	<i>passim</i>
<i>Biosig Instruments, Inc. v. Nautilus, Inc.</i> , 783 F.3d 1374 (Fed. Cir. 2015).....	6
<i>Citrix Sys, Inc. v. Workspot, Inc.</i> , No. 18-588, 2020 WL 5634219 (D. Del. 2020).....	11, 15
<i>Dropbox, Inc. v. Motion Offense, LLC</i> , 2022 WL 174519 (W.D. Tex. 2022).....	10
<i>Dyfan, LLC v. Target Corp.</i> , 28 F.4th 1360 (Fed. Cir. 2022)	11, 16, 17
<i>Ericsson Inc. v. TCL Commc’n. Tech. Holdings, Ltd.</i> , 161 F. Supp. 3d 438 (E.D. Tex. 2015).....	15
<i>Estech Sys., Inc. v. Burnco Texas LLC</i> , No. 2:20-CV-00275-JRG-RSP, 2021 WL 2530959 (E.D. Tex. June 18, 2021).....	13
<i>Hill–Rom Servs., Inc. v. Stryker Corp.</i> , 755 F.3d 1367 (Fed. Cir. 2014).....	3
<i>In re Teles AG Informationstechnologien</i> , 747 F.3d 1357 (Fed. Cir. 2014).....	16, 17
<i>Intel Corp. v. Qualcomm Inc.</i> , 21 F.4th 784 (Fed. Cir. 2021)	14, 19
<i>JVW Enterprises, Inc. v. Interact Accessories, Inc.</i> , 424 F.3d 1324 (Fed. Cir. 2005).....	16
<i>KCJ Corp. v. Kinetic Concepts, Inc.</i> , 223 F.3d 1351 (Fed. Cir. 2000).....	9
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014).....	7, 17-19

<i>Netfuel, Inc. v. F5 Networks, Inc.</i> , 2017 WL 2834538 (N.D. Ill. 2017)	15
<i>Pitney Bowes, Inc. v. Hewlett–Packard Co.</i> , 182 F.3d 1298 (Fed. Cir. 1999).....	3, 4
<i>Salazar v. AT&T Mobility LLC</i> , 64 F.4th 1311 (Fed. Cir. 2023)	9
<i>Samsung Elecs. Am., Inc. v. Prisua Eng’g Corp.</i> , 948 F.3d 1342 (Fed. Cir. 2020).....	13
<i>Sectra Comms AB v. Absolute Software Inc.</i> , 2023 WL 4106279 (W.D. Wash. 2023).....	15
<i>Starhome Gmbh v. AT&T Mobility LLC</i> , 743 F.3d 849 (Fed. Cir. 2014).....	3
<i>Thorner v. Sony Computer Entm’t Am. LLC</i> , 669 F.3d 1362 (Fed. Cir. 2012).....	<i>passim</i>
<i>Williamson v. Citrix Online, LLC</i> , 792 F.3d 1339 (Fed. Cir. 2015).....	11
<i>WSOU Investments LLC v. Google LLC</i> , 2023 WL 6889033 (Fed. Cir. Oct. 19, 2023).....	11, 13
<i>Zeroclick, LLC v. Apple Inc.</i> , 891 F.3d 1003 (Fed. Cir. 2018).....	13, 15, 16
STATUTES	
35 U.S.C. §112, Sixth Paragraph	<i>passim</i>

I. INTRODUCTION

Plaintiff Softex LLC (“Softex”) respectfully submits this responsive brief in support of its proposed constructions for the disputed claim terms in U.S. Patent Nos. 7,590,837 (“’837 patent”), 8,516,235 (“’235 patent”), 8,145,892 (“’892 patent”), 8,287,603 (“’603 patent”), 8,506,649 (“’649 patent”), 8,137,410 (“’410 patent”), and 8,128,710 (“’710 patent”) (collectively, the “Asserted Patents”).¹ Softex’s proposed constructions are consistent with the claim language interpreted in light of the intrinsic record. Absolute Software Corporation and Absolute Software, Inc. (“Defendants” or “Absolute”) consistently seek to rewrite claims by injecting unnecessary language through proposed claim constructions that are inconsistent with the intrinsic record. Further, Defendants fail to prove by clear and convincing evidence that the claims do not inform with reasonable certainty those skilled in the art about the scope of the invention.

II. THE PATENTED TECHNOLOGY

The Asserted Patents share a common specification and relate to systems for securing and tracking an electronic device. *See* ’837, Abstract, 1:34-38. The Asserted Patents disclose an electronic device security and tracking system and method (ESTSM). *Id.* Such a system and method may comprise “a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device.” *Id.*, 1:34-42; *see also* Rubin Declaration (“Ex. A”) at ¶¶30-56.

For example, the systems of the ’837 patent increase the effectiveness of theft prevention by using a combination of a basic input/output system (BIOS) component, a non-viewable component, and an application component, working in conjunction with one another to provide a

¹ All lettered exhibits cited herein, Exhibits A to K to the Declaration of Christina A. Ondrick (“Ondrick Decl.”), filed herewith.

persistent theft detection security solution. *Id.*, 2:12-17. These systems allow the application component to cause a stolen electronic device to send a message containing the location information of the electronic device to the server system. *Id.*, 8:23-53. Further, the BIOS component ensures the ESTSM application cannot be tampered with, bypassed, or removed from the electronic device. *Id.*, 17:62-64. The BIOS component “check[s] the integrity of the ESTSM non-viewable component and application component programs and files, and restore[s] the original programs and files, if they have been tampered with.” *Id.*, 17:64-18:8. The BIOS component ensures that the application component ran “properly on the previous device boot” and will take action if it is determined that an attempt to bypass the application component has occurred.” *Id.*, 18:8-12. The non-viewable component determines if the application component is present and if the application component was tampered with. *Id.*, 26:31-27:3. Thus, users thwart thieves who attempt to remove or alter the theft prevention and recovery software.

III. ARGUMENT

A. “basic input/output system (BIOS)” / “BIOS”

The dispute regarding these terms is narrow. Appx. 1. The parties agree that a BIOS is “firmware that is used to start the computer system after it is powered on.” Br. 15 (conceding that the BIOS is firmware used to start the computer once powered on); Ex. K, 150:21-25. Consistent with Softex’s proposal and Defendants’ concession, the specification explains that the BIOS “enable[s] the computer to load the operating system software program into main memory during system initialization and transfer control to the operating system so the operating system can start executing” the boot sequence. ’837, 21:65-22:2; *see also* Ex. D, 85; Ex. A, 59-71.

Defendants wrongly attempt to add at least the following unnecessary structural and functional limitations into the claim language: that the BIOS must be stored in read-only memory (“ROM”), supports data transfer among hardware devices, and is a set of essential software

routines that tests hardware at startup. Each of these extraneous limitations goes well beyond the plain meaning of the BIOS term and should be rejected. Ex. A, 57-71.

“The starting point for any claim construction must be the claims themselves.” *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999). Nothing in the claim language suggests that the BIOS is stored in read-only memory, supports data transfer among hardware devices, or is a set of essential software routines that tests hardware at startup. Ex. A, 59-71, 227-245. The Defendants’ proposed construction should be rejected because it departs from the plain meaning of the claim language. The Federal Circuit has emphasized that it will “indulge a heavy presumption that a claim term carries its customary and ordinary meaning” as understood by a person of ordinary skill in the relevant field or art. *E.g.*, *Starhome GmbH v. AT&T Mobility LLC*, 743 F.3d 849, 857 (Fed. Cir. 2014). Moreover, the precedent is clear that a court should “depart from the plain and ordinary meaning of claim terms based on the specification in *only two* narrow instances: *lexicography* and *disavowal*.” *E.g.*, *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1371 (Fed. Cir. 2014) (emphasis added). Further, these precedents underscore the rigor of these exceptions, noting they are “exacting” and not readily met. *Id.* This is because it is improper to read structural or functional limitations into the claims. Defendants’ proposed constructions should not be accepted because no evidence of lexicography or disavowal exists. *Thorner v. Sony Computer Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

ROM not required: Defendants argue that the BIOS *must* be stored on a ROM. Br. 16. Dr. Cullimore admitted that was not the case in his deposition. Ex. K, 154:15-155:21. The intrinsic record also refutes Defendants’ argument; nothing in the intrinsic record *requires* the use of only ROM. Ex. A, 59-60. To the contrary, it was well-known at the time of the invention that the

BIOS could be stored on many types of memory, including flash memory. *Id.*, 62-66 (citing Exs. B to E). Therefore, a POSITA would understand that a ROM is *neither* a requirement nor a defining characteristic of the claimed BIOS. *Id.*

No Data Transfer Support Among Unspecified Hardware Devices or Set of Essential Software Routines: Defendants argue that the BIOS must support data transfer among undefined “hardware devices” and include an undefined “set of essential software routines” to “test” undefined hardware at startup. Defendants’ sole basis for this proposal is extrinsic evidence relating to “PC-compatible computers” on Windows and IBM machines Ex. 9 at 60 (Windows); *see also* Ex. 7 at 44 (IBM), Ex. 11 (BIOS for IBM PCs). The Asserted Patents are not limited to Windows and IBM machines. ’837, 2:12-24 (discussing a Windows machine, a DOS machine, a Linux machine, and others). Nothing in the claim language (or the specification) requires IBM or Windows PCs or the unnecessary language urged by Defendants. Simply put, where the intrinsic record unambiguously describes the scope of the patented invention, reliance on any extrinsic evidence is improper. *See Pitney Bowes*, 182 F.3d at 1308.

B. “power on self test (POST)”

The Court need not construe “power on self test (POST)” because the term is self-explanatory. Appx. 1. Further, the patents contain neither claim scope disavowal nor lexicography. *Thorner*, 669 F.3d at 1365; Ex. A, 73-82. The specification explains that the POST “firmware may call the ESTSM BIOS component 5310 towards the end of POST.” ’837, 24:62-64. If the “ECA information is correct (i.e., ESTSM application was run correctly),” then the “POST” proceeds with the boot process. *Id.*, 25:41-44. Dr. Rubin also confirms that POST has a plain and ordinary meaning to a POSITA. Ex. A, 73-82. A BIOS typically includes a test referred to as a POST that ensures that the computer can boot up properly. *Id.*, 74. Computers initiate this operation after being turned on and before booting the operating system. *Id.*

In contrast to Softex’s plain and ordinary meaning proposal, Defendants’ proposed construction wrongly seeks to add extraneous limitations to the claim. Specifically, the Defendants’ proposed construction improperly specifies *where* the POST is stored (ROM). Ex. K, 163:2-4. But, as discussed above, nothing in the patent requires that the BIOS be stored on a ROM. Therefore, the POST—a part of the BIOS—is likewise not required to be stored on a ROM. Ex. A, 78.

The mistake in Defendants’ proposal is exposed by a plain reading of the claim language. Specifically, the claim specifies what happens if “problems are not found,” i.e., “proceed with powering up the electronic device.” Defendants’ construction, in contrast, seeks to add the additional functional limitations that “if problems are found, alert the user.” *Nothing* in the claim language suggests what happens if problems *are* found, and the intrinsic record, yet again, contains no evidence warranting the insertion of these limitations. *Thorner*, 669 F.3d at 1368; Ex. K, 164:15-22.

Defendants’ proposed construction seeks to add yet additional extraneous limitations, seeking to add “a set of routines” that “test various system components” to “see whether they are properly connected and operating.” Again, nothing in the intrinsic record mandates adding these additional functional requirements into the claimed POST. *Id.*, 163:2-165:7. The term requires no construction because a POSITA would have understood this term’s plain and ordinary meaning. Ex. A, 82.

C. “hidden partition”

“[A] patent claim is indefinite if, when ‘read in light of the specification delineating the patent, and the prosecution history, [the claim] fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention.’” *BASF Corp. v. Johnson Matthey Inc.*, 875 F.3d 1360, 1365 (Fed. Cir. 2017) (alterations in original). If “a person of ordinary skill in the art,

with the aid of the specification [and prosecution history], would understand what is claimed, the claim is not indefinite.” *Biosig Instruments, Inc. v. Nautilus, Inc.*, 783 F.3d 1374, 1381 (Fed. Cir. 2015). Indefiniteness is a challenge to the validity of a patent and must be shown by clear and convincing evidence. *BASF Corp.*, 875 F.3d at 1365.

Defendants have not come close to meeting the high burden of proving indefiniteness. Their expert concedes that the idea of a hidden partition was known at the time of the invention. Ex. K, 166:10-15. Also, the claims clearly instruct what a hidden partition is. Beyond this, the specification explains that the “creation of the ESTSM hidden partition may be performed immediately after the electronic device’s hard disk drive is installed. Various utilities can be used to create the hidden partition” ’837, 31:26-29. Consistent with that observation, almost every modern computer has a hidden partition used for recovery and one of ordinary skill in the art would have no trouble understanding what is claimed. Ex. A, 84-96 (citing Exs. G to I). Confirming the well-understood meaning, Defendants use the term “hidden partition” on their websites to describe a hidden memory partition for system recovery. *Id.* Defendants even cite prior art that refers to a “hidden disk partition.” Br. 16.

Dr. Rubin explained in his declaration that any POSITA would have understood—with reasonable certainty—what a hidden partition means. Ex. A, 84-96. In contrast, Dr. Cullimore report simply argues in a conclusory fashion that the term is ambiguous regarding who the partition is hidden from. Cullimore, 202-03. In any event, Dr. Cullimore is incorrect and admitted that hidden partitions were well-understood in his deposition. Ex. K, 166:10-15. A partition is either hidden, or it is not. And here, as set forth above and explained by Dr. Rubin (and Defendants’ websites and Defendants’ brief), hidden partitions are *not* “hidden from all users at all times.” Br. 17. A hidden partition is simply a partition that is not visible under normal

conditions. Ex. A, 90, 93. In sum, this term is far from indefinite and should be given its plain and ordinary meaning without any special construction. Appx. 1.

D. “operating correctly” / “operated correctly”

Defendants have not met their burden of proving by clear and convincing evidence that the “operating correctly” terms “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). Considering the full intrinsic record, the claim language is more than sufficient for any POSITA to understand “the scope of the invention.” *BASF*, 875 F.3d at 1365; Ex. A, 98-104.

Starting with the claim language, claim 1 of the ’410 patent (for example) recites determining whether an application component “operated correctly.” The specification teaches that the “ESTSM application was run correctly” if “the ECA information is correct.” ’410, 26:2-3. If the application components fail to run correctly (e.g., the ECA information is missing or incorrect), “the electronic device will be disabled....” *Id.*, 26:5-10. As can be seen from the plain language of the intrinsic record, the scope of the invention is clear. Indeed, the inventive concept of the ’410 patent recognizes that a thief may delete or tamper with the ESTSM. Because of this recognition, any time there is an effort to “prevent the ESTSM from running,” then “[a]n application component failure will be generated.” *Id.*, 26:5-20; *see also id.*, 18:65-67 (deleting application files to prevent the application from running), 18:67-19:12 (preventing the application files from running on every boot will result in not booting the system), Fig. 54. Defendants thus incorrectly argue that the specification fails to inform a POSITA how to distinguish whether an application component “operated correctly.”

In contrast, the Defendants’ proposed construction is supported only by a dictionary definition devoid of the context of the specification. Elevating extrinsic evidence over intrinsic

evidence is neither necessary nor appropriate where, as here, an analysis of the intrinsic evidence alone resolves any ambiguity in the disputed claim term. *Phillips*, 415 F.3d at 1318.

Given the specifications’ consistent and repeat disclosures, Dr. Rubin explained that one of skill in the art would understand—with reasonable certainty—the meaning and scope of the “operating correctly” terms to mean operating as expected. Appx. 1, 2, Ex. A, 98-104. As Dr. Rubin explains, an application component is not “operating correctly” if it is supposed to run on every boot and fails to do so. If, on the other hand, the application component is supposed to run on every boot, and it does, then it is “operating correctly.” *Id.*, 101-02. Dr. Cullimore agreed in his deposition. Ex. K, 180:4-14. There is nothing indefinite about these claim terms.

E. The “wherein integrating” terms

The Defendants’ indefiniteness argument here relies upon a misrepresentation of the claims. Specifically, Defendants contend that the claims require the ESTSM image to “configure the device to have” a claimed component that can be deleted. Br. 18. Based on this sleight of hand, Defendants argue that the BIOS does not know “which applications may run *after* it executes.” *Id.* Defendants’ inaccurate description of the claim language cannot form the basis for clear and convincing evidence of indefiniteness. Appx. 2.

The claims provide that “integrating the ESTSM ROM image into the BIOS” configures “the electronic device for having” three components. ’235, claims 1-7, 15-21. The specification teaches exactly how to integrate the ESTSM ROM image into the BIOS such that the device is configured “for having” functionality *during the BIOS execution*. Ex. A, 106-17 (citing Figs. 62a, 63 and corresponding disclosures); *see also* Ex. K at 182:18-185:3 (agreeing). The image enables calling the BIOS component at the end of the POST. Ex. A, 106-17. The BIOS component transfers control to the non-viewable component, which determines if the application

component ran correctly during the last system boot and, if so, the POST proceeds with the boot process. *Id.* Thus, the image configures the device “for” having the claimed components.

Considering the full intrinsic record, the claim language is more than sufficient for a POSITA to understand “the scope of the invention.” *BASF*, 875 F.3d at 1365; Ex. A, 117. The Court should reject the Defendants’ invalidity argument. The plain language should govern.

F. “primary server”/ “central server”

The “primary server”/“central server” terms are entitled to their plain and ordinary meaning. Appx. 2, 3. Defendants seek to limit the claim terms to **one particular** server. Br. 19 (arguing claim terms require the “same primary server” or “a particular server”); *see also id.*, 20 (making the same line of argument for the “central server”); Ex. K, 189:10-15, 195:2-6 (Dr. Cullimore’s opinion is nothing more than an instruction from counsel). But Defendants’ proposed constructions are manifestly incorrect and not supported by the intrinsic record.

The claims recite “a primary server” or “a central server,” therefore, these terms should be given their plural meaning of one or more primary/central servers. The Federal Circuit has “repeatedly emphasized that an indefinite article ‘a’ or ‘an’ in patent parlance carries the meaning of ‘one or more’ in open-ended claims,” like the asserted claims here. *See, e.g., KCJ Corp. v. Kinetic Concepts, Inc.*, 223 F.3d 1351, 1356 (Fed. Cir. 2000). The subsequent use of the definite article “the” “to refer back to the same claim term does not change the general plural rule, but simply reinvoles that non-singular meaning.” *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342-43 (Fed. Cir. 2008). Thus, the claim terms “a primary server/a central server” are not properly restricted to only one primary/central server. And the subsequent limitations referring to “the primary server/the central server” are references back to the one or more primary/central servers. *Salazar v. AT&T Mobility LLC*, 64 F.4th 1311, 1315 (Fed. Cir. 2023). Nothing in the claim language or specification identifies a manifest disavowal of the

plural-allowing meaning of “a primary server/a central server” here. *ABS Glob., Inc. v. Cytonome/St, LLC*, 84 F.4th 1034, 1040-41 (Fed. Cir. 2023). Instead, the Asserted Patents explain that the application component communicates with multiple servers. ’837, 17:49-55; Ex. A, 106-17.

Defendants’ reliance on the specification as limiting fails because Figure 52 is identified as nothing more than “one embodiment of the invention.” ’837, 6:11-14. Defendants also contend that the claimed servers cannot refer to the “cloud” because the cloud “was not available until approximately 2006.” Br. 20. That is simply incorrect. Ex. A, 127-131 (citing Ex. J (the term was used in 1996, and the idea is from the 1960s); *see also* Ex. K at 193:11-15 (Dr. Cullimore agreeing that the idea of the cloud was known in the 1980s). Critically, cloud is a marketing term and a metaphor for the Internet, which predated the Asserted Patents. Ex. A, 129 (citing Ex. J, 2). The specification is clear: the application communicates with servers through the Internet. *Id.*, 119-121; *see also* Ex. K, 192:19-194:12 (Dr. Cullimore agreeing); ’837, 17:51-55; Fig. 44 (the server is a “number of servers” that may be “web servers containing the web pages and data for ESTSM”).

G. “changeable area” / “system area” / “non-volatile storage device” / “non-volatile memory”

The Court should adopt Softex’s proposed claim constructions for these terms, which Softex proposed but Defendants failed to address. Defendants waived all arguments regarding these terms. *See Dropbox, Inc. v. Motion Offense, LLC*, 2022 WL 174519, *8 (W.D. Tex. 2022) (collecting cases to explain that “[a]rguments raised for the first time in a reply brief are waived.”). The Court should adopt Softex’s proposed constructions. Appx. 35

H. The Component/Module Terms

1. 35 U.S.C. §112, Sixth Paragraph, Does Not Apply

Established precedent makes clear that a §112, sixth paragraph, analysis “asks two questions. First: Is the disputed claim limitation drafted in means-plus-function format? Second, if and only if the answer to the first question is ‘yes’: What, if any, is the structure corresponding to the claimed function?” *Dyfan, LLC v. Target Corp.*, 28 F.4th 1360, 1367 (Fed. Cir. 2022). Here, since the disputed component/module terms do not use the word “means” there is a rebuttable presumption that the claims do not invoke §112, sixth paragraph. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015) (*en banc* in relevant portion). To overcome this presumption, Defendants must show, by “a preponderance of the evidence,” that a POSITA would not have understood the component/module limitations, as claimed, “to connote structure *in light of the claim as a whole*.” *Dyfan*, 28 F.4th at 1367 (emphasis added).

In determining whether claim limitations recite sufficient structure, courts look beyond the “component” and “module” terms and to the intended functionality of the component/module to determine if a person of ordinary skill would have understood the claim limitation as a whole to connote sufficiently definite structure. *WSOU Investments LLC v. Google LLC*, 2023 WL 6889033, at *5 (Fed. Cir. Oct. 19, 2023) (“[C]laim limitations like the recited ‘computer program code,’ when combined with a description of what the code is intended to accomplish, convey definite structure to the ordinarily skilled artisan”); *see also Citrix Sys, Inc. v. Workspot, Inc.*, No. 18-588, 2020 WL 5634219, *8-11 (D. Del. 2020) (Judge Stark finding component and module terms not subject to §112, sixth paragraph).

Claims and Specification: Turning to the claims themselves, the language does not merely recite a “module” or “component,” as Defendants’ argument suggests. Br. 3, 4. For example, claim 1 of the ’837 patent specifically recites how the application component, non-

viewable security component, BIOS security component and validator module operate in conjunction with one another and what they are intended to accomplish while also providing structural limitations, such as the BIOS security component is stored in a secure area of non-volatile memory. In this example, claim 1 of the 837 patent (and similarly claim 5 of the '235 patent) recites “a non-viewable security component in the electronic device, wherein the non-viewable security component comprises a validator module capable of determining whether the application component is present and whether the application component has been tampered with.” The remaining claims similarly recite the operational algorithm of these claimed features using different syntax. *See, e.g.*, Ex. A, 155-58 (applicant component); 183-86 (non-viewable [security] component); 227-28 (BIOS [security] component).

The specification confirms that the claims (and the terms) inherently require a programmed processor. *See, e.g.*, Fig. 44 (showing the relevant module and components), 49 (showing the hardware), 53 (processor programmed with the BIOS [security] component), 54 (processor programmed with the validator module / non-viewable [security] component), 55 (processor programmed with the application component). As Dr. Rubin explains, like the claims, the entirety of the specification describes the invention in the context of a specially programmed computer. Ex. A, 155-178 (application component), 183-204 (non-viewable [security] component), 210-220 (validator module), 225-46 (BIOS[security] component).

Dr. Rubin confirms all of this by explaining that the specification describes the operation of the claimed components and module in the context of a programmed computer processor, detailing their interactions with other programmed components and modules in the ESTSM system. *Id.*, 163, 185, 212, 227. As such, a POSITA would have understood that programmed computers, like those described in the specification, are necessarily implemented via computer

circuitry, including a processor and memory. All of this connotes specific structure, and § 112, sixth paragraph, does not apply. *WSOU*, 2023 WL 6889033, at *5.

A POSITA's Understanding of the Claims and Specification: As Dr. Rubin explains, a POSITA would have understood from these disclosures that the claims require a programmed computer to perform the claimed functions. Ex. A, 163, 185, 213, 227; *Estech Sys., Inc. v. Burnco Texas LLC*, No. 2:20-CV-00275-JRG-RSP, 2021 WL 2530959, at *7 (E.D. Tex. June 18, 2021). When read in this context, the claim-recited components/module refer to a broad class of operational computer program structures. Ex. A, 26, 27, 144-51. As explained by Softex's expert, Dr. Rubin, a person of ordinary skill would have understood the terms as a particular structure and claimed limitations as a whole to connote sufficiently definite structure after analyzing the functional language in the record. *Id.*; *WSOU*, 2023 WL 6889033, at *5.

Beyond that, the claims themselves provide significant indicia of structure by reciting *how* these components interact to achieve the computer security features of the inventions. Ex. A, 144-51. The Federal Circuit has found that claimed recitations of how components interact to achieve a claim-recited objective provides sufficient indicia of structure to maintain the presumption against § 112, sixth paragraph. *See, e.g., Zeroclick, LLC v. Apple Inc.*, 891 F.3d 1003, 1008 (Fed. Cir. 2018) (“program that can [perform function]” found to be sufficiently definite structure in part because the claims provided operational context for the program).

The Federal Circuit has held that terms that “clearly serve[] as a stand-in for a ‘general purpose computer’ or a ‘central processing unit’” connote sufficient “structure” and avoid § 112 ¶ 6. *Samsung Elecs. Am., Inc. v. Prisia Eng'g Corp.*, 948 F.3d 1342, 1354 (Fed. Cir. 2020) (“As used in the claims of the '591 patent, the term ‘digital processing unit’ clearly serves as a stand-in for a ‘general purpose computer’ or a ‘central processing unit,’ each of which would be

understood as a reference to structure in this case, not simply any device that can perform a particular function.”). Here, the intrinsic and extrinsic evidence all confirm that the disputed terms discussed in this section serve as a stand-in for a programmed general-purpose computer or a central processing unit, so § 112, sixth paragraph, does not apply. *Id.*; Ex. A, 163, 185, 213, 227. The Court should reject the Defendants’ invitation to commit legal error and conclude that the programmatic component/module terms are *not* governed by §112, sixth paragraph.

Defendants Improperly Focus on Extrinsic Evidence and Fail to Consider Whether There Was Existing Code for Performing the Claimed Functions: Rather than addressing the intrinsic evidence, Defendants and their expert offer conclusions rather than evidence. Br. 6-15. For example, Defendants’ proposed constructions rely upon the flawed proposition that the claim can be dissected into individual words, e.g., “validator” and “module,” wholly devoid of context. Br. 14-15; Ex. K, 144:18-145:21 (Defendants looked to only extrinsic evidence); *see also id.* 141:6-144:17 (same for non-viewable component terms), 147:11-150:1 (same for BIOS component and application component terms). But that approach is improper. *Intel*, 21 F.4th at 792.

Defendants also contend that “there is no algorithm or other structure disclosed in the specification” for the claimed functionality. Br., 13, 15. This contention is patently incorrect. As explained in §III.D, the specification clearly explains that the validator module determines whether the application ran correctly on the last boot. *See also* similar discussions for the other terms in §§III.H.3.a-c. Therefore, Defendants have not established that § 112, sixth paragraph, applies. As explained in §III.H.3, Softex’s plain and ordinary constructions should be adopted.

Ignoring the intrinsic record, Defendants fall back on extrinsic evidence to assert that the words “module” and “component” are “meaningless.” Br., 3-4. The extrinsic evidence that

Defendants cite to—including statements from Dr. Cullimore, excerpts from technical dictionaries, and other patents—fails to account for the full context of the claim language and instead wrongly focuses *exclusively* on the words “component” and “module” in a vacuum. Br., 3-4. Defendants’ constructions are improper and contrary to the law for failing to examine the claimed “component” and “module” in the full context of the intrinsic record. *Zeroclick*, 891 F.3d at 1008.

The failings in Defendants’ §112, sixth paragraph positions are confirmed by the findings of numerous courts that claims including “component” or “module” carry a plain and ordinary meaning. *See, e.g., Citrix Sys., Inc.*, *8-11; *Ericsson Inc. v. TCL Commc’n. Tech. Holdings, Ltd.*, 161 F. Supp. 3d 438, 445-52 (E.D. Tex. 2015); *Netfuel, Inc. v. F5 Networks, Inc.*, 2017 WL 2834538, *3-8 (N.D. Ill. 2017). In a separate case against Absolute involving similar technology, the court concluded that Absolute’s proposed construction of a “[first/second] software component” “needlessly over-describes the term, which is already understandable to a POSA and needs no construction.” *Sectra Comms AB v. Absolute Software Inc.*, 2023 WL 4106279, *5 (W.D. Wash. 2023).

Defendants’ Expert Admitted That He Never Considered Whether Existing Code Was Present for Performing Claimed Functions: The Federal Circuit also instructs that the courts should look to whether the disputed terms are used “as specific references to conventional ... code, existing in prior art at the time of the inventions.” *Zeroclick*, 891 F.3d at 1008. When viewed through this lens, Defendants did not come close to rebutting the presumption against application §112, sixth paragraph. Critically, the Defendants’ expert never considered whether existing code was present for performing the claimed functions of the disputed terms. Ex. K, 98:25-109:14 (Dr. Cullimore did not form an opinion about whether the application component,

BIOS [security] component, non-viewable [security] component, or validator module could be implemented with existing code). Beyond that failing, Defendants themselves have contended, in invalidity contentions, that these terms reference conventional, publicly disclosed components/modules existing at the time of the invention. *See generally* Ex. K at Ex. 2. Defendants cannot overcome the presumption against § 112, sixth paragraph. *Dyfan*, 28 F.4th at 1369; *Zeroclick*, 891 F.3d at 1008.

2. If the Court Finds That §112, Sixth Paragraph, Does Apply:

a) The Court Should Adopt Softex’s Proposals

The component and module terms do not invoke § 112, sixth paragraph. But, if the Court finds that it does apply, Softex’s identified functions and structures should be adopted. Softex properly proposed the “claimed” functions and the corresponding structures from the specifications to perform the claimed functions. Ex. A, 180, 206, 247. Defendants did not.

b) Defendants’ Proposals are Facially Incorrect

“[A] court may not construe a means-plus-function limitation by adopting a function *different from that explicitly recited in the claim.*” *JVW Enterprises, Inc. v. Interact Accessories, Inc.*, 424 F.3d 1324, 1331 (Fed. Cir. 2005). When construing claims under § 112, ¶ 6, “[t]he statute does not permit limitation of a means-plus-function claim by adopting a function different from that explicitly recited in the claim.” *In re Teles AG Informationstechnologien*, 747 F.3d 1357, 1367-68 (Fed. Cir. 2014). As such, a court cannot adopt unclaimed functions from a working embodiment disclosed in the written description. *JVW Enters.*, 424 F.3d at 1331.

Defendants’ proposed constructions must be rejected because they included functions *different* from those claimed. Rather than analyzing the component terms on a claim-by-claim basis, Defendants combine claimed functionality across several claims and patents. In doing so, Defendants’ Frankenstein-like construction proposes the wrong functionality for *every*

component term. Ex. A, 180, 206, 247. For example, the application component in claim 1 of the '837 patent performs different functions from the application component in claim 1 of the '892 patent, but the Defendants' proposed construction wrongly combines the functions.

Defendants' citation to *Frank's Casing* is inapposite, as that case involved claim terms in different claims where the claimed functions were the same. Br. 5. In contrast, the component terms here have *different* claimed functions. Thus, it would be an error to incorporate "unrecited functional limitations into the [various] claims." *In re Teles* 747 F.3d at 1367-68.

Finally, because Defendants' "no corresponding structure argument" (Br. 6-7) relies on an incorrect identification of corresponding functions, Defendants' "no corresponding structure" argument fails as a matter of law. *Dyfan*, 28 F.4th at 1367.

3. No Claim Term Is Indefinite

a) "application component"

Defendants have also not met their burden of proving by clear and convincing evidence that the "application component" terms "fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus*, 572 U.S. at 901; Br. 13. Considering the full intrinsic record, the claim language is more than sufficient for a POSITA to understand "the scope of the invention." *BASF*, 875 F.3d at 1365; Ex. A, 153-178.

Starting with the claim language, the application components provide operational context. *See, e.g.*, '837, cl 1. ("cause the electronic device to send, to the server system, a message that contains location information," "determine whether the electronic device has been reported stolen, based on information received from the server system"); *see also* cl. 1 of the other Asserted Patents.

The plain language of the intrinsic record demonstrates there is nothing indefinite about these terms, and the scope of the invention is clear. Indeed, the patented concept recognizes that

the application component communicates with the server to facilitate the ESTSM. Ex. A, 178. This understanding is supported by the specification (e.g., Fig. 55 and corresponding disclosures). The specification teaches, for example, an “application component” that is part of a software application that “runs within the operating system environment and is responsible for communicating with the ESTSM server computer system 4465 through the Internet 4475.” ’837, 17:45-52, Fig. 44. Given these clear disclosures, Dr. Rubin explained that one of skill in the art would readily understand—with reasonable certainty—the meaning and scope of the “application component” terms. Ex. A, 155-78; Appx. 3.

In contrast, the Defendants’ proposed construction should be rejected because it is supported solely by extrinsic evidence. Ex. K, 149:11-150:1. Resorting to extrinsic evidence is neither necessary nor appropriate where, as here, an analysis of the intrinsic evidence alone resolves any ambiguity in the disputed claim term. *Phillips*, 415 F.3d at 1318.

b) “non-viewable [security] component”

Defendants have not met their burden of proving by clear and convincing evidence that these terms are indefinite. *Nautilus*, 572 U.S. at 901; *BASF*, 875 F.3d at 1365; Br. 8-9; Ex. A, 181-204. Again, the surrounding claim language provides additional context to these terms that the Defendants ignore. Ex. K, 141:6-144:17. Defendants’ failure to analyze the surrounding words of the claims dooms the argument. *Phillips*, 415 F.3d at 1314, 1321 (Although the claims themselves provide substantial guidance as to the meaning of particular claim terms, the context of the surrounding words of the claim also must be considered. “[T]he ordinary meaning of a claim term is its meaning to the ordinary artisan after reading the entire patent.”).

For example, the claimed “non-viewable security component” includes “a validator module capable of determining whether the application component is present and whether the application component has been tampered with.” 837, cl. 1; *see also*, e.g., 410, cl. 1. The

specification further provides that a non-viewable component is a part of a computer program that is not viewable and/or hidden. '837, 2:12-55, 18:3-65, 19:26-53. Softex's expert, Dr. Rubin, explains that a POSITA would have understood that the purpose of making the component non-viewable would be to hide it from a normal/typical user such that the ESTSM could operate securely without the user noticing. Ex. A, 181-204.

Defendants' argument that the "non-viewable [security] component can be identified by drawing a metaphorical box around *any part* of a computer program" highlights Defendants' attempt to construe these terms in a vacuum devoid of context, thus violating fundamental tenets of claim construction. Br. 8, 9. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 792 (Fed. Cir. 2021) (the "inquiry is not limited to an analysis of the phrase in isolation" but rather, claim construction "demands interpretation of the entire claim in context, not a single element in isolation.").

Finally, Defendants' proposed construction of these terms as "a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive" again seeks to import limitations not required by the claim language. Br. 8, 9. Defendants' extraneous "hidden partition or Host Protected Area" limitation need not be added to the plain meaning of the claim term because *nothing* in the claim language or specification mandates such a narrow reading. *Thorner*, 669 F.3d at 1368. The Court should adopt Softex's proposed claim construction, which is "a part of a [security-related] computer program, the contents of which are not viewable to a typical or normal user." Appx. 15, 16.

c) "BIOS [security] component" (and corresponding terms)

Defendants' proposed term chart contends that these terms are "indefinite" under 35 U.S.C. §112, first paragraph. Appx 22-35. But, by not presenting and thereby waiving that argument in their brief, Defendants have not carried their burden for proving indefiniteness. *Nautilus*, 572 U.S. at 901. Beyond this, Defendants mischaracterize Softex's proposal as "a

computer application” as part of a strawman attack. Br., 12. In short, this is not Defendants’ proposed construction and Defendants’ mischaracterization should be ignored. Appx 22-35.

These terms should be given their plain and ordinary meaning, which is “[security] component of electronic device firmware that is used to start the computer system after it is powered on.” Ex. A, 224-45. As discussed above, in §III.A (BIOS term), Softex’s proposals are supported by the claims and specifications. Defendants’ contrary proposals are incorrect for the same reasons discussed above in §III.A (BIOS term). Ex. K, 147:11-149:4. Beyond this, Defendants’ proposal reads out the word “security” for the BIOS security terms, leaving the BIOS component and BIOS security component with identical constructions. This cannot be correct. Similarly, Defendants, unnecessarily burden every term with “option ROM BIOS image in an extension ROM BIOS.” It is inappropriate to rewrite the claims to include an option ROM BIOS image in an extension ROM BIOS when *nothing* in the claim language suggests such a narrow reading, and the intrinsic record provides no evidence of lexicography or disavowal. *Thorner*, 669 F.3d at 1368.

d) “validator module”

Defendants do not contend this term is indefinite under 35 U.S.C. §112, first paragraph. Appx. 21. Further, Defendants only offer means-plus-function construction for this term. Thus, to the extent the Court finds that this is not a means-plus-function term, which it is not as discussed above, Softex’s proposed plain and ordinary meaning construction, which is a computer application that validates—stands unchallenged. Br. 14, 15.

IV. CONCLUSION

For the foregoing reasons, Softex respectfully requests this Court adopt Softex’s proposed claim constructions and reject Defendants’ claim constructions and indefiniteness arguments.

Dated: November 28, 2023

Respectfully submitted,

McKool Smith, P.C.

/s/ Blair M. Jacobs

Blair M. Jacobs (WDTX. Bar No. 32010)

bjacobs@McKoolSmith.com

Christina A. Ondrick (WDTX. Bar No. 494625)

condrick@McKoolSmith.com

John S. Holley (SBN 24078678)

jholley@McKoolSmith.com

1999 K Street, NW Suite 600

Washington, D.C. 20006

Telephone: (202) 370-8300

Facsimile: (202) 370-8344

John B. Campbell (SBN 24036314)

jcampbell@McKoolSmith.com

McKool Smith, P.C.

303 Colorado Street, Suite 2100

Austin, TX 78701

Telephone: (512) 692-8700

Facsimile: (512) 692-8744

Casey L. Shomaker (SBN 24110359)

cshomaker@McKoolSmith.com

Matthew Folks (SBN 24116368)

mfolks@McKoolSmith.com

McKool Smith, P.C.

300 Crescent Court, Suite 1500

Dallas, TX 75201

Telephone: (214) 978-4218

Facsimile: (214) 978-4044

***ATTORNEYS FOR PLAINTIFF
SOFTEX LLC***

APPENDIX OF PROPOSED CONSTRUCTIONS

Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
“basic input/output system (BIOS)” / “BIOS” / “Basic Input/Output System (BIOS)” <ul style="list-style-type: none"> • ’837 patent claims 1-3, 8-14, 18; • ’235 patent claims 1-21; ’892 patent claims 1-19; • ’603 patent claims 1-4, 10, 12-14, and 18-20; • ’410 patent claims 15-20; • ’710 patent claims 1-8, 11-21, 23 	Plain and ordinary meaning, which is electronic device firmware that is used to start the computer system after it is powered on.	the set of essential software routines that tests hardware at startup, starts the operating system, supports the transfer of data among hardware devices, and is stored in read-only memory (ROM) so that it can be executed when the computer is turned on
Term / Claims	Softex's Proposed Construction	Defendants' Proposed Construction
power on self test (POST) <ul style="list-style-type: none"> • ’410 patent claims 1-4, 7-11, and 14-20 	No construction necessary, plain and ordinary meaning.	“A set of routines stored in a computer’s read-only memory (ROM) that tests various system components such as RAM, the disk drives, and the keyboard to see whether they are properly connected and operating and, if problems are found, alert the user or, if problems are not found, pass control to the system’s bootstrap loader to load the operating system”
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
hidden partition <ul style="list-style-type: none"> • ’837 patent claim 23; • ’410 patent claims 1-4, 7-11, 14-20 	No construction necessary - plain and ordinary meaning	Indefinite Alternatively, if not indefinite: “a hard drive partition that is hidden to all users”
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
operating correctly / operated correctly	Plain and ordinary meaning, which is operating/operated as expected.	Indefinite

<ul style="list-style-type: none"> • '410 patent claims 1-4, 7-11, and 14-20; • '603 patent claims 1-4, 10, 12-14, and 18-20 		
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
<p>“wherein integrating the ESTSM ROM image into the BIOS of the electronic device configures the electronic device for having a non-viewable component, an application component connected to the non-viewable component and capable of executing within an operating system environment and of communicating with the non-viewable component, and a BIOS component connected to the non-viewable component” /</p> <p>“wherein integrating the ESTSM ROM image into the BIOS of the electronic device configures the electronic device for having a non-viewable component, an application component that is connected to the non-viewable component, that is capable of communicating with the non-viewable component, and that executes within an operating system environment”</p> <ul style="list-style-type: none"> • '235 patent claims 1-7, 15-21 	No construction necessary, plain and ordinary meaning.	Indefinite
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
<p>primary server</p> <ul style="list-style-type: none"> • '603 patent claims 2-4, 13-14, and 19-20 	No construction necessary, plain and ordinary meaning.	“a particular server that is the first server with which the user's device attempts to communicate”

Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
central server <ul style="list-style-type: none"> '710 patent claim 1 	No construction necessary, plain and ordinary meaning.	"a particular server located within the premises of the administrator of the electronic device security system"
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
If §112, sixth paragraph, does not apply		
application component <ul style="list-style-type: none"> '837 claims 1-3, 5-14, and 16-27; '235 claims 1-21; '892 claims 1-19; '603 claims 1-4, 10-14, and 18-20; '410 claims 1-4, 7-11, and 14-20; '710 claims 1-8, 11-21, 23 	Not subject to § 112, ¶ 6, no construction necessary.	Indefinite under § 112, ¶ 1
Term	Softex's Proposed Construction	Defendants' Proposed Construction
'837 Patent Claim 1 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claim 1 (function):</u></p> <ul style="list-style-type: none"> configured to cause the electronic device to send, to the server system, a message that contains location information for the electronic device; to determine whether the electronic device has been reported stolen, based on information received from the server system; to notify the BIOS security component that the electronic device has been reported stolen, in response to 	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has</p>

	<p>determining that the electronic device has been reported stolen.</p> <p><u>Claim 1 (structure):</u> a computer application configured to to perform the sending, determining and notifying disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 18:66-19:2; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67; 26:57-64; 33:26-29.</p>	<p>been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server"</p> <p><u>Structure:</u> Indefinite (no structure disclosed)</p>
'837 Patent Claims 12, 20 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 12, 20 (function):</u></p> <ul style="list-style-type: none"> • configured to cause the electronic device to send, to the server system, a message that contains location information for the electronic device, and • capable of determining whether the electronic device has been reported stolen, based on information received from the server system <p><u>Claims 12, 20 (structure):</u> a computer application configured to perform the sending and determining disclosed in Figs.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been</p>

	40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67.	<p>reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server"</p> <p>Structure: Indefinite (no structure disclosed)</p>
'235 Patent Claims 1, 4 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claim 1, 4 (function):</u></p> <ul style="list-style-type: none"> capable of communicating with the non-viewable component, send, to the server system, a message that contains information of a location of the electronic device, and configured to determine whether the electronic device has been reported stolen, based on information received from the server system. <p><u>Claims 1, 4 (structure):</u> a computer application configured to perform the communicating, sending and determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 18:66-</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a</p>

	19:2; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67; 26:57-64; 33:26-29.	<p>communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p> <p>Structure: Indefinite (no structure disclosed)</p>
'235 Patent Claim 6 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p>Claims 4, 11, 18 (function):</p> <ul style="list-style-type: none"> to cause the electronic device to send, to the server system, a message that contains information of a location of the electronic device, and to determine whether the electronic device has been reported stolen, based on information received from the server system. <p>Claims 4, 11, 18 (structure): a computer application configured to perform the sending and determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the</p>

		<p>device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server"</p> <p>Structure: Indefinite (no structure disclosed)</p>
'235 Patent Claim 7 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claim 7 (function):</u></p> <ul style="list-style-type: none"> configured to notify the BIOS component that the electronic device has been reported stolen, in response to determining that the electronic device has been reported stolen. <p><u>Claim 7 (structure):</u> a computer application configured to perform the notifying disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 18:66-19:2; 25:63-67; 26:57-64;</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server</p>

		<p>system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p> <p>Structure: Indefinite (no structure disclosed)</p>
'235 Patent Claims 8, 15 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p>Claims 8, 15 (function):</p> <ul style="list-style-type: none"> communicating with the non-viewable component <p>Claims 8, 15 (structure): a computer application configured to perform the communicating disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 17:39-42; 18:41-46; 18:66-19:2; 25:63-67; 26:57-64;</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile</p>

		<p>storage device in response to an instruction from the server”</p> <p>Structure: Indefinite (no structure disclosed)</p>
'235 Patent Claims 14, 21 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 14, 21 (function):</u></p> <ul style="list-style-type: none"> to notify the BIOS component that the electronic device has been reported stolen, in response to determining that the electronic device has been reported stolen. <p><u>Claims 14, 21 (structure):</u> a computer application configured to perform the notifying disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 18:66-19:2; 19:34-40; 19:62-67; 21:50-55; 25:37-41; 26:17-22.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p>

		Structure: Indefinite (no structure disclosed)
'892 Patent Claims 1, 11, 12, 15 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 11, 12, 15 (function):</u></p> <ul style="list-style-type: none"> communicating with the non-viewable component, and that is capable of communicating through a secure medium with a server system <p><u>Claims 1, 11, 12, 15 (structure):</u></p> <p>a computer application configured to perform the communicating disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 18:66-19:2; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67; 26:57-64; 33:26-29.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p>

		Structure: Indefinite (no structure disclosed)
'603 Patent Claims 1, 12, 18 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 12, 18 (function):</u></p> <ul style="list-style-type: none"> to automatically ascertain whether the electronic device has been reported stolen, based on information received from a server system. <p><u>Claims 1, 12, 18 (structure):</u> a computer application configured to perform automatic ascertaining disclosed in Figs. 40; 42; 44; 45; 46; 47; 48; 49; 55, 71; 72; 15:25-30; 15:61-66; 33:65-34:4; 34:13-20; 34:58-67.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p> <p>Structure: Indefinite (no structure disclosed)</p>

'410 Patent Claims 1, 8, 15 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 8, 15 (function):</u></p> <ul style="list-style-type: none"> associated with tracking and locating the electronic device <p><u>Claims 1, 8, 15 (structure):</u></p> <p>a computer application configured to perform automatic ascertaining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 11:4-9; 15:25-37; 15:63-67; 16:15-17; 17:65-17:1; 19:20-25; 19:29-31; 20:17-27; 24:33-44.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p> <p><u>Structure:</u> Indefinite (no structure disclosed)</p>
'710 Patent Claims 1, 2, 19 (if §112, sixth paragraph does apply)		

application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 2, 19 (function):</u></p> <ul style="list-style-type: none"> capable of communicating with the non-viewable component <p><u>Claims 1, 2, 19 (structure):</u> a computer application configured to perform the communicating disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 17:39-42; 18:41-46; 18:66-19:2; 25:63-67; 26:57-64</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p> <p><u>Structure:</u> Indefinite (no structure disclosed)</p>
'710 Patent Claim 13 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p>

	<p><u>Claim 13 (function):</u></p> <ul style="list-style-type: none"> record that the electronic device has been reported stolen, after the report that the electronic device has been stolen has been received <p><u>Claim 13 (structure):</u> a computer application configured to perform the recording disclosed in Figs. 40; 42; 44; 45; 46; 47; 48; 49; 55, 71; 72; 15:25-30; 15:61-66; 33:65-34:4; 34:13-20; 34:58-67.</p>	<p><u>Function:</u> “provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device’s location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server”</p> <p><u>Structure:</u> Indefinite (no structure disclosed)</p>
’710 Patent Claim 15 (if §112, sixth paragraph does apply)		
application component	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claim 15 (function):</u></p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p><u>Function:</u> “provide security and tracking for an electronic device; communicate</p>

	<ul style="list-style-type: none"> • erase the non-volatile storage device in response to an instruction from the server system <p><u>Claim 15 (structure):</u> a computer application configured to perform the recording disclosed in Figs. 42, 44, 45, 55; 2:28-34; 8:41-47; 14:21-25; 15:59-63; 16:2-5; 17:55-61; 23:35-38; 26:57-61.</p>	<p>through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server"</p> <p><u>Structure:</u> Indefinite (no structure disclosed)</p>
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
§112, sixth paragraph does not apply		
non-viewable component <ul style="list-style-type: none"> • '235 patent claims 1-21; • '892 patent claims 1-19; • '410 patent claims 1-4, 7-11, 14-20; 	"a part of a computer program, the contents of which are not viewable to a typical or normal user."	Indefinite under § 112, ¶ 1

<ul style="list-style-type: none"> '710 patent claims 1-8, 11-21, 23 		
Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction
§112, sixth paragraph does not apply		
non-viewable security component <ul style="list-style-type: none"> '837 patent claims 1-3, 5-14, and 16-27 	"a part of a security-related computer program, the contents of which are not viewable to a typical or normal user."	Indefinite under § 112, ¶ 1
'235 Patent Claims 1, 5, 8, 12, 15, and 19 (if §112, sixth paragraph, applies)		
non-viewable component	<p>Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6:</p> <p><u>Claims 1, 5, 8, 12, 15, and 19 (function):</u> determine whether the application component is present and whether the application component has been tampered with</p> <p><u>Claims 1, 5, 8, 12, 15, and 19 (structure):</u> a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: "track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with"</p>

		<p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive”</p>
'892 Patent Claims 1, 11, 12, 15 (if §112, sixth paragraph, applies)		
non-viewable component	<p>Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6:</p> <p><u>Claims 1, 11, 12, 15 (function):</u> determine whether the application component is present and whether the application component has been tampered with</p> <p><u>Claims 1, 11, 12, 15 (structure):</u> a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: “track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with”</p>

		<p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive”</p>
'410 Patent Claims 1, 8 (if §112, sixth paragraph, applies)		
non-viewable component	<p>Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6:</p> <p><u>Claims 1, 8, (function):</u></p> <ul style="list-style-type: none"> • automatically determining whether the application component operated correctly during last power-up of the electronic device; • in response to a determination that the application component did not operate correctly during last power-up of the electronic device, automatically restoring the application component from a backup fileset; and • automatically placing the electronic device under control of power on self test (POST) to proceed with powering-up the electronic device in response to a determination that the application component operated correctly during last power-up of the electronic device. <p><u>Claims 1, 8 (structure):</u></p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with”</p>

	a computer application configured to perform the determining disclosed in Figs. 54, 55; 2:49-52; 19:35-40; 25:31-49; 25:63-26:3; 26:12-22.	<p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive”</p>
'410 Patent Claim 15 (if §112, sixth paragraph, applies)		
non-viewable component	<p>Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6:</p> <p><u>Claim 15 (function):</u></p> <ul style="list-style-type: none"> associated with tracking and locating the electronic device <p><u>Claim 15 (structure):</u> a computer application configured to perform the determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 11:4-9; 15:25-37; 15:63-67; 16:15-17; 17:65-17:1; 19:20-25; 19:29-31; 20:17-27; 24:33-44.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: “track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with”</p>

		<p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive”</p>
'837 Patent Claims 1-3, 8-14, 18-24 (if §112, sixth paragraph, applies)		
non-viewable security component	<p>Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6:</p> <p><u>Claims 1, 5, 8, 12, 15, and 19 (function):</u> determining whether the application component is present and whether the application component has been tampered with</p> <p><u>Claims 1, 5, 8, 12, 15, and 19 (structure):</u> A computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: “track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with”</p>

		Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: Structure: “a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive”
Term(s) / Claim(s)	Softex’s Proposed Construction	Defendants’ Proposed Construction
§112, sixth paragraph does not apply		
validator module <ul style="list-style-type: none"> ’837 patent claims 1-3, 8-14, 18-24; ’235 patent claims 5, 12, and 19 	Not subject to § 112, ¶ 6, plain and ordinary meaning, which is “a computer application that validates”	No construction offered
’837 Patent Claims 1, 12, 20 (if §112, sixth paragraph, applies)		
validator module	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: <u>Claims 1, 12, and 20 (function):</u> <ul style="list-style-type: none"> determining whether the application component is present and whether the application component has been tampered with <u>Claims 1, 12, and 20 (structure):</u> a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.	Invokes 35 U.S.C. § 112, ¶ 6: Function: “determine whether an application component is present and whether the application component has been tampered with” Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: Structure: “a program that implements the steps shown in Figure 54”
’235 Patent Claims 5, 12, 19 (if §112, sixth paragraph, applies)		
validator module	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6:	Invokes 35 U.S.C. § 112, ¶ 6:

	<p><u>Claims 5, 12, and 19 (function):</u> determine whether the application component is present and whether the application component has been tampered with</p> <p><u>Claims 5, 12, and 19 (structure):</u> a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.</p>	<p>Function: “determine whether an application component is present and whether the application component has been tampered with”</p> <p>Structure: Indefinite (no structure disclosed)</p> <p>Alternatively, if not indefinite under ¶ 6: Structure: “a program that implements the steps shown in Figure 54”</p>
Term(s) / Claim(s)	Softex’s Proposed Construction	Defendants’ Proposed Construction
§112, sixth paragraph does not apply		
<p>“BIOS component” / “basic input/output system (BIOS) component”</p> <ul style="list-style-type: none"> • ’235 patent claims 1-21; • ’892 patent claims 1-19; • ’603 patent claims 1-4, 10, 12-14, and 18-20; • ’410 patent claims 15-20; • ’710 patent claims 1-8, 11-21, 23 	Not subject to § 112, ¶ 6, plain and ordinary meaning, which is “component of electronic device firmware that is used to start the computer system after it is powered on.”	<p>Indefinite under § 112, ¶ 1</p> <p>Alternatively, if not indefinite under ¶ 1: “a BIOS ROM image in an option ROM BIOS”</p>
<p>Basic input/output system (BIOS) security component” / “BIOS security component”</p> <ul style="list-style-type: none"> • ’837 patent claims 1-3, 8-14, 18-24 • ’892 patent claims 11-14 	Not subject to § 112, ¶ 6, plain and ordinary meaning, which is “security component of electronic device firmware that is used to start the computer system after it is powered on.”	<p>Indefinite under § 112, ¶ 1</p> <p>Alternatively, if not indefinite under ¶ 1: “a BIOS ROM image in an option ROM BIOS”</p>
’235 Patent Claims 1, 8, 15 (if §,112 sixth paragraph, applies)		
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:	Invokes 35 U.S.C. § 112, ¶ 6:

	<p><u>Claims 1, 8, 15 (function):</u></p> <ul style="list-style-type: none"> • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with, • check integrity of the application component during a boot process for the electronic device, • automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component <p><u>Claims 1, 8, 15 (structure):</u> a computer application configured to perform the determining, checking and causing disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.</p>	<p>Function: “track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen”</p>
--	--	---

		<p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
'235 Patent Claims 13, 20		
BIOS component terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 13, 20 (function):</u></p> <ul style="list-style-type: none"> prevent the electronic device from booting to an operating system of the electronic device, in response to receiving notification that the electronic device has been reported stolen <p><u>Claims 13, 20 (structure):</u> a computer application configured to perform the preventing in Figures 53, 54, 55, 71; 3:32-35; 18:59-61; 18:65-19:5; 19:23-30; 19:34-48; 19:43-48; 20:13-23; 26:13-50.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: “track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device</p>

		<p>under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen”</p> <p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
'892 Patent Claims 1, 11, 12, 15		
BIOS component terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 11, 12, 15 (function):</u></p> <ul style="list-style-type: none"> determine whether the non-viewable component is present and whether the 	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot</p>

	<p>non-viewable component has been tampered with,</p> <ul style="list-style-type: none"> • check integrity of the application component during a boot process for the electronic device, • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component <p><u>Claims 1, 11, 12, 15 (structure):</u> a computer application configured to perform the determining, checking and causing disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.</p>	<p>process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen”</p> <p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of</p>
--	--	---

		the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”
’603 Patent Claims 1, 12, 18		
BIOS component terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 12, 18 (function):</u></p> <ul style="list-style-type: none"> automatically preventing the electronic device from completing the boot process if the BIOS component does not find the information from the application component indicating that the application component was operating correctly <p><u>Claims 1, 12, 18 (structure):</u> a computer application configured to perform the preventing in Figures 53, 54, 55, 71; 3:32-35; 18:59-61; 18:65-19:5; 19:23-30; 19:34-48; 19:43-48; 20:13-23; 26:13-50.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: “track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application</p>

		<p>component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen”</p> <p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
'410 Patent Claim 15		
BIOS component terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 15 (function):</u></p> <ul style="list-style-type: none"> • automatically determining whether the application component operated correctly during last power-up of the electronic device; • in response to a determination that the application component did not operate correctly during last power-up of the electronic device, automatically restoring the application component from a backup fileset; and 	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of</p>

	<ul style="list-style-type: none"> • automatically placing the electronic device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the electronic device. <p><u>Claim 15 (structure):</u> a computer application configured to perform the determining, restoring and placing disclosed in Figures 53, 53, 54, 55, 71; 3:1-16; 17:61-18:12; 18:37-46; 18:59-61; 19:43-48; 20:13-23; 24:62-67; 25:41-62; 26:13-50.</p>	<p>the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen”</p> <p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
’710 Patent Claims 1, 2, 19		

<p>BIOS component terms</p>	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 2, 19 (function):</u></p> <ul style="list-style-type: none"> • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with, • check integrity of the application component during a boot process for the electronic device, • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component <p><u>Claims 1, 2, 19 (structure):</u> a computer application configured to perform the determining, checking and causing disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6: Function: “track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen”</p>
-----------------------------	--	---

		<p>Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
'837 Patent Claims 1, 12		
BIOS Security Component Terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 1, 12 (function):</u></p> <ul style="list-style-type: none"> • check integrity of the application component during a boot process for the electronic device; • determine whether the non-viewable security component is present and whether the non-viewable security component has been tampered with; • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check for the application component; • prevent the electronic device from booting to the OS, in response to receiving notification that the electronic device has been reported stolen; 	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for the electronic device; check integrity of an application component during a boot process for the device; determine whether a non-viewable security component is present and whether it has been tampered with; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check for the application component; automatically cause the device to reinstall the application component from a hidden partition of a hard disk drive, in response to a negative integrity check for the application component; prevent the device from booting to an OS, in response to receiving notification that the device has been reported stolen; prevent the device”</p>

	<p><u>Claims 1, 12 (structure):</u> a computer application configured to perform the checking, determining, causing, and preventing disclosed in Figures 53, 54, 55, 71; 3:1-16; 3:32-35; 18:4-8; 18:37-46; 19:23-30; 19:34-48; 19:43-48; 20:13-23; 26:13-50; 26:65-27:3.</p>	<p>from booting to the OS, in response to receiving notification that the device is to be disabled; cause the device to respond to a negative integrity check for the application component by using a backup copy of the application component to restore the integrity of the application component; locate the device; disable the device; and track the device until the device is disabled”</p> <p>Structure: Indefinite (no structure disclosed)</p> <p>Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
'837 Patent Claim 20		
BIOS Security Component Terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 20 (function):</u></p> <ul style="list-style-type: none"> check integrity of the application component during a boot process for the electronic device; 	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for the electronic device; check integrity of an application component during a boot process for the device; determine whether a non-viewable security component is present and whether it has been tampered</p>

	<ul style="list-style-type: none"> • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check for the application component; • determine whether the non-viewable security component is present and whether the non-viewable security component has been tampered with <p><u>Claims 20 (structure):</u> a computer application configured to perform the checking, causing, and determining disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 18:59-61; 18:65-19:5; 19:43-48; 20:13-23; 26:13-50.</p>	<p>with; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check for the application component; automatically cause the device to reinstall the application component from a hidden partition of a hard disk drive, in response to a negative integrity check for the application component; prevent the device from booting to an OS, in response to receiving notification that the device has been reported stolen; prevent the device from booting to the OS, in response to receiving notification that the device is to be disabled; cause the device to respond to a negative integrity check for the application component by using a backup copy of the application component to restore the integrity of the application component; locate the device; disable the device; and track the device until the device is disabled”</p> <p>Structure: Indefinite (no structure disclosed)</p> <p>Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in</p>
--	--	--

		associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”
’892 Patent Claims 11, 12		
BIOS Security Component Terms	<p>Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:</p> <p><u>Claims 11, 12 (function):</u></p> <ul style="list-style-type: none"> • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with, • check integrity of the application component during a boot process for the electronic device, and • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component, <p><u>Claims 11, 12 (structure):</u> a computer application configured to perform the checking, causing, and determining disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.</p>	<p>Invokes 35 U.S.C. § 112, ¶ 6:</p> <p>Function: “provide security and tracking for the electronic device; check integrity of an application component during a boot process for the device; determine whether a non-viewable security component is present and whether it has been tampered with; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check for the application component; automatically cause the device to reinstall the application component from a hidden partition of a hard disk drive, in response to a negative integrity check for the application component; prevent the device from booting to an OS, in response to receiving notification that the device has been reported stolen; prevent the device from booting to the OS, in response to receiving notification that the device is to be disabled; cause the device to respond to a negative integrity check for the application component by using a backup copy of the application component to restore the integrity of the application component; locate the device; disable the</p>

		<p>device; and track the device until the device is disabled”</p> <p>Structure: Indefinite (no structure disclosed)</p> <p>Alternatively, if not indefinite under ¶ 6:</p> <p>Structure: “a BIOS ROM image in an option ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification”</p>
Term(s) / Claim(s)	Softex’s Proposed Construction	Defendant’s Proposed Construction
changeable area <ul style="list-style-type: none"> • ’649 patent claims 1, 7, 9, 15 	Plain and ordinary meaning, which is an area of computer memory that can be modified	
Term(s) / Claim(s)	Softex’s Proposed Construction	Defendant’s Proposed Construction
“system area” <ul style="list-style-type: none"> • ’649 patent claims 1, 7, 9, 15 	Plain and ordinary meaning, which is an area of computer memory that cannot be modified	
Term(s) / Claim(s)	Softex’s Proposed Construction	Defendant’s Proposed Construction
“non-volatile storage device” <ul style="list-style-type: none"> • ’837 patent claims 1-3, 8-14, 18; • ’710 patent claims 1-8, 11-21, 23 	Plain and ordinary meaning, which is memory that persists in its state when the power is removed	
Term(s) / Claim(s)	Softex’s Proposed Construction	Defendant’s Proposed Construction
“non-volatile memory” <ul style="list-style-type: none"> • ’649 patent claims 1, 7, 9, 15 	Plain and ordinary meaning, which is memory that persists in its state when the power is removed	

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the above and foregoing document has been served on all counsel of record through the Court's CM/ECF system on November 28, 2023.

/s/ Blair M. Jacobs
Blair M. Jacobs